Matthew R. Wilson (SBN 290473)
mwilson@meyerwilson.com
Jared W. Connors *(Pro Hac Vice forthcoming)*
jconnors@meyerwilson.com
MEYER WILSON CO., LPA
305 W. Nationwide Boulevard
Columbus, OH 43215
Telephone: (614) 224-6000
Facsimile: (614) 224-6066

M. Anderson Berry (SBN 262879)
aberry@justice4you.com
Gregory Haroutunian (SBN 330263)
gharoutunian@justice4you.com
CLAYEO C. ARNOLD,
A PROFESSIONAL CORPORATION
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916)239-4778
Fax: (916) 924-1829

John J. Nelson (SBN 317598)
jnelson@milberg.com
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
401 W Broadway, Suite 1760
San Diego, California 92101
Telephone: (858) 209-6941

[Additional Counsel on signature page]

Attorneys for Plaintiffs and the Proposed Class

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

IN RE: SAN FRANCISCO 49ERS DATA BREACH LITIGATION	Case No. 3:22-cv-05138
This Document Relates To:	**FIRST AMENDED CONSOLIDATED CLASS ACTION COMPLAINT**
ALL ACTIONS	**DEMAND FOR JURY TRIAL**

Plaintiffs Samantha Donelson, Kathrine Finch, James Sampson ("Plaintiffs") through their attorneys, brings this Consolidated Class Action Complaint against the Defendant, Forty Niners Football Company LLC ("the 49ers" or "Defendant"), alleging as follows:

I. INTRODUCTION

1. From February 6 to February 11, 2022, the San Francisco 49ers, a National Football League franchise based in the greater San Francisco Bay Area, lost control over at least 20,000 individuals' highly sensitive personal information in a data breach ("Data Breach"), and then failed to notify those individuals about the breach for over six months.

2. Cybercriminals bypassed the 49ers' inadequate security systems using ransomware to access individuals' personally identifiable information ("PII"), including their names, dates of birth, and Social Security numbers. The cybercriminals also accessed information regarding the employees' immigration statuses and their dependents' PII.

3. From February 6 to February 11, 2022, cybercriminals breached the 49ers' "corporate IT network" and impacted its operations. It is unknown for how long the breach went undetected, meaning the 49ers had no effective means to prevent, detect, or stop the Data Breach from happening before cybercriminals stole and misused PII.

4. Despite public news reports of the incident, it was not until August 9, 2022, that the 49ers' investigation confirmed the unauthorized access to PII stored in its system. Instead of alerting its affected individuals immediately, as required under California law, the 49ers did not disclose the breach until August 31, 2022.

5. On August 31, 2022, the 49ers finally informed affected individuals of the Data Breach and offered them just 12 months of free credit monitoring service, which fails to adequately address the lifelong threat the Data Breach poses to impacted individuals.

///

6. The 49ers' failures to adequately protect PII stored in its systems and timely notify those affected about the devastating Data Breach harms its current and former employees in violation of California law.

7. Plaintiffs are all victims of the Data Breach, and they bring this action on behalf of themselves and all others harmed by the 49ers' misconduct, seeking relief on a class wide basis.

8. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion and to timely notify Plaintiffs and Class Members in the event of a Data Breach.

9. Defendant failed to adequately protect Plaintiffs' and Class Members' PII and seemingly failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect the sensitive, non-public data it maintained for its own pecuniary benefit. Hackers targeted and obtained Plaintiffs' and Class Members' PII because of its value in exploiting and stealing the identities of Plaintiffs and Class Members. As a result of Defendant's failure to implement adequate data security protocols, the risk of fraud and identity theft to impacted individuals will remain for their respective lifetimes.

10. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts, at least, to negligence and violates federal and state statutes.

///

11. Plaintiffs and Class Members have suffered injuries as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and (iv) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

12. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that the PII of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they are entitled to injunctive and other equitable relief.

II. PARTIES

13. Plaintiff Samantha Donelson, is a natural person and citizen of Georgia, residing in Atlanta, Georgia, where she intends to remain. Plaintiff Donelson received Notice of Data Breach dated August 31, 2022, shortly after that date. If Plaintiff Donelson had known that Defendant would not adequately protect her PII, she would not have allowed Defendant access to this sensitive and private information.

14. Plaintiff Kathrine Finch is a resident and citizen of California, currently residing in Garden Grove, California. Plaintiff Finch received Defendant's Notice of Data Breach, dated August 31, 2022, shortly after that date. If Plaintiff Finch had known that Defendant would not adequately protect her PII, she would not have allowed Defendant access to this sensitive and private information.

15. Plaintiff James Sampson is a resident and citizen of California, currently residing in Oakland, California. Mr. Sampson received Defendant's Notice of Data Breach, dated August 31, 2022, shortly after that date. If Mr. Sampson had known that Defendant would not adequately protect his PII, he would not have allowed Defendant access to this sensitive and private information.

16. Defendant 49ers Enterprises, LLC dba the San Francisco 49ers is a Delaware corporation registered to do business in California, with its principal place of business at 4949 Marie P. Debartolo Way, Santa Clara, California 95054.

III. JURISDICTION & VENUE

17. This Court has jurisdiction over Plaintiffs' claims under 28 U.S.C. § 1332(d)(2) because there are over 1,000 class members, Ms. Donelson is a citizen of a different state than the 49ers, and the aggregate amount in controversy for the class exceeds $5 million, exclusive of interest and costs.

18. This Court has personal jurisdiction over Defendant because the 49ers are registered to do business and is headquartered in California and is subject to this Court's general and specific jurisdiction and this cause of action arises out of events that took place in California.

19. Venue is proper in this District under 28 U.S.C. §§ 1391 because a substantial part of the events or omissions giving rise to the claims emanated from activities within this District and Defendant is headquartered in this District.

IV. BACKGROUND FACTS

The 49ers

20. The San Francisco 49ers have been a franchise in the National Football League since 1950, having won five Super Bowl championships in the eighties and early nineties. Since 2014, the 49ers have been based in and around Levi's Stadium in Santa Clara, California.

21. As part of its business operations, the 49ers store PII on its employees, vendors, and other business partners. This information, including names, dates of birth, and Social Security Numbers, was stored on the 49ers internal corporate IT systems.

22. Despite the obvious sensitivity of this information, the 49ers apparently did not implement reasonable cybersecurity safeguards or policies to protect PII, or trained its employees to prevent, detect, and stop data breaches of the 49ers' systems. As a result, the 49ers leave vulnerabilities in its systems for cybercriminals to exploit and give access to PII.

23. In collecting and maintaining the PII, the 49ers implicitly agree it will safeguard the data using reasonable means according to its internal policies and state and federal law.

24. Despite its duties to safeguard PII, on February 6, 2022, cybercriminals bypassed the 49ers' security systems undetected and accessed PII as part of a "ransomware" attack.

25. As of at least February 13, 2022,[1] there were public reports that the 49ers were subject to a ransomware attack. Despite these reports, the 49ers did not immediately inform affected or potentially affected individuals about the breach or otherwise notify them according to California law. Instead, the 49ers initiated an internal investigation to "identify the individuals

[1] https://www.cnn.com/2022/02/13/us/49ers-network-security-incident/index.html (last accessed Mar. 24, 2023).

whose information was contained in the files."[2] This investigation, according to the 49ers, took until August 9, 2022. During the investigation, the 49ers did not contact any of the affected individuals.

26. On information and belief, the currently unidentified cybercriminals utilized a type of ransomware called "BlackByte" to penetrate the 49ers' systems. In fact, BlackByte listed the 49ers on its website as a system successfully penetrated by the program.[3]

27. On August 31, 2022, the 49ers finally notified affected individuals of the Data Breach ("Breach Notice")— nearly six months after the Data Breach.[4]

28. Despite "investigating" the Data Breach for several months, the 49ers' Breach Notice revealed little about the breach and obfuscated its nature. The 49ers' Breach Notice assures affected individuals that "We take this situation seriously," telling them that the 49ers is "taking steps to prevent something like this from occurring again, including additional measures to further enhance our security protocols and continued education and training to our employees"—steps that should have taken place *before* the Data Breach.

29. The 49ers' Breach Notice informs Data Breach victims they can sign up for 12 months of free credit monitoring, which does not adequately address the lifelong harm that the Data Breach poses to its victims.

30. The 49ers' Breach Notice does not explain how the hack happened, why it took so long for the 49ers to discover it, what exactly cybercriminals stole, and why it took the 49ers nearly

---

[2] https://oag.ca.gov/system/files/SF%2049ers%20-%20California%20Notification.pdf (last accessed Mar. 24, 2023).

[3] *See* https://www.cnn.com/2022/02/13/us/49ers-network-security-incident/index.html (last accessed Mar. 24, 2023).

[4] https://oag.ca.gov/ecrime/databreach/reports/sb24-556853 (last accessed Mar. 24, 2023).

6 months to disclose the breach in a bare-bones notice.

31. On information and belief, the 49ers failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over PII it stored in its systems. The 49ers' negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing PII.

32. By obtaining, collecting, and storing the PII of Plaintiff Donelson and the Class, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

33. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiff and the Class.

Plaintiff Samantha Donelson's Experience

34. Plaintiff Samantha Donelson is an employee of the Atlanta Falcons, another franchise in the NFL.

35. Ms. Donelson works for the Falcons in their live events department. As part of her work for the Falcons, Ms. Donelson provided her information to the 49ers.

36. Plaintiff Donelson provided her PII to the 49ers and trusted that the company would use reasonable measures to protect it according to the 49ers internal policies, as well as state and federal law.

37. As a result of a previous data breach, Plaintiff Donelson utilized Credit Wise, a credit monitoring service provided via Capital One.

38. In February 2022—soon after the 49ers breach—Credit Wise informed Plaintiff Donelson that her Social Security number had been used on the "dark web." On information and belief, the "dark web" is an internet portal where compromised identities can be traded or sold by cybercriminals.

///

39. At the time, Plaintiff Donelson had no way to connect this incident to the 49ers Data Breach, and no substantive information regarding who was affected was available.

40. Plaintiff Donelson has and will spend considerable time and effort monitoring her accounts to protect herself from identity theft.

41. On September 5, 2022, Plaintiff Donelson received notice from the 49ers that her name, date of birth, and Social Security Number was compromised as part of the Data Breach.

42. Plaintiff Donelson suffered actual injury and damages due to Defendant's failure to secure and safeguard her PII before the Data Breach.

43. Plaintiff Donelson suffered actual injury in the form of damages and diminution in the value of her PII—a form of intangible property that she entrusted to Defendant as part of her job duties in the NFL organization.

44. Plaintiff Donelson has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her stolen PII, especially her Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

45. Plaintiff fears for her personal financial security and uncertainty over what PII was exposed in the Data Breach. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

46. Plaintiff Donelson has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

///

Plaintiff Kathrine Finch's Experience

47. Plaintiff Kathrine Finch was an employee of an NFL franchise and was required to provide and did provide her PII to Defendant.

48. Plaintiff Finch typically takes measures to protect her private information and is very careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

49. Plaintiff Finch stores any documents containing her PII in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for her online accounts.

50. Shortly after August 31, 2022, Plaintiff Finch received the Notice from Defendant informing her that her PII had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff's PII, including her name, date of birth, and Social Security number, was compromised as a result of the Data Breach.

51. As a result of the Data Breach, and at the direction of Defendant's Notice letter, Plaintiff Finch made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to, researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching the credit monitoring and identity theft protection services offered by Defendant and private companies. Plaintiff Finch has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation.

52. Plaintiff Finch suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Defendant obtained from Plaintiff Finch; (b) violation of her privacy rights; and (c) present, imminent and impending injury arising from the increased

risk of identity theft and fraud.

53. As a result of the Data Breach, Plaintiff Finch anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Finch is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come. Plaintiff and Class Members will need identity theft protection services and credit monitoring services for their respective lifetimes, considering the immutable nature of the PII at issue, which includes Social Security numbers.

Plaintiff James Sampson's Experience

54. Plaintiff James Sampson was required to provide and did provide his PII to Defendant.

55. Plaintiff Sampson typically takes measures to protect his private information and is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

56. Plaintiff Sampson stores any documents containing his PII in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for his online accounts.

57. Shortly after August 31, 2022, Plaintiff received the Notice from Defendant informing him that his PII had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Sampson's PII, including his name, Social Security number, and payment information, was compromised as a result of the Data Breach.

58. After, and as a result of the Data Breach, Plaintiff Sampson has experienced at least two fraudulent purchases on the same credit card used to make purchases with Defendant (and exposed in the Data Breach as alleged herein).

59. As a result of the Data Breach, and at the direction of Defendant's Notice letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not

limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching the credit monitoring and identity theft protection services offered by Defendant. Plaintiff has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation.

60. Plaintiff suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from Plaintiff; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

61. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiffs and the Proposed Class Face Significant Risk of Continued Identity Theft

62. Plaintiffs and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

63. As a result of the 49ers' failure to prevent the Data Breach, Plaintiffs and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered, or are at an increased risk of suffering:

i. The loss of the opportunity to control how their PII is used;

ii. The diminution in value of their PII;

iii. The compromise and continuing publication of their PII;

iv. Out-of-pocket costs associated with the prevention, detection, recovery, and

remediation from identity theft or fraud;

v. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

vi. Delay in receipt of tax refund monies;

vii. Unauthorized use of stolen PII; and

viii. The continued risk to their PII, which remains in the possession of defendant and is subject to further breaches so long as defendant fails to undertake the appropriate measures to protect the PII in their possession.

64. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

65. The value of Plaintiffs' and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

66. It can take victims years to stop identity or PII theft, giving criminals plenty of time to use that information for cash.

67. One such example of criminals using PII for profit is the development of "Fullz" packages.

68. Cybercriminals can cross-reference two sources of PII to marry unregulated data

available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

69. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cybercriminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs and other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

70. Defendant disclosed the PII of Plaintiffs and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiffs and members of the proposed Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

71. Defendant's failure to properly notify Plaintiffs and members of the proposed Class of the Data Breach exacerbated Plaintiffs and members of the proposed Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

///

///

Defendant Violated the FTC Act

72. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

73. The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

74. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

i. protect the personal customer information that they keep;

ii. properly dispose of personal information that is no longer needed;

iii. encrypt information stored on computer networks;

iv. understand their network's vulnerabilities; and

v. implement policies to correct security problems.

75. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

76. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security

measures. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

77. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

V. CLASS ACTION ALLEGATIONS

78. Under Fed.R.Civ.P. 23, Plaintiffs sue on behalf of themselves and the proposed Class ("Class"), defined as follows:

> All individuals whose PII was compromised in the Data Breach disclosed by the San Francisco 49ers on or about August 31, 2022.
> about August 31, 2022 ("Nationwide Class" or "Class").
>
> All individuals residing in California whose PII was compromised in the data breach first announced by Defendant on or about August 31, 2022 (the "California Subclass").
>
> All individuals residing in Georgia whose PII was compromised in the data breach first announced by Defendant on or about August 31, 2022 (the "Georgia Subclass").

79. Collectively the Class, California Subclass, and Georgia Subclass are referred to as Classes or Class.

80. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

81. Plaintiffs reserve the right to amend the class definition.

82. **Ascertainability.** The 49ers have identified, or are able to identify, all individuals affected by the data breach. These records will identify the Class Members.

83. **Numerosity.** The class includes approximately 20,000 class members, so individual joinder would be impracticable.

84. **Commonality and Predominance.** This case presents questions of law and fact common to all class members, and those common questions predominate over individualized issues. These common questions include:

1. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiffs and the Class's PII;
2. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
3. Whether Defendant was negligent in maintaining, protecting, and securing PII;
4. Whether Defendant breached contractual promises to safeguard Plaintiffs' and the Class's PII;
5. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;
6. Whether Defendant's Breach Notice was reasonable;
7. Whether the Data Breach caused Plaintiffs' and the Class injuries;
8. What the proper damages measure is; and
9. Whether Plaintiffs and the Class are entitled to damages, treble damages, or injunctive relief.

///

///

85. **Typicality**. Plaintiffs' claims are typical of Class member's claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

86. **Adequacy**. Plaintiffs will fairly and adequately protect the proposed Class's interests. Her interests do not conflict with Class members' interests, and she has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

87. **Superiority**. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individuals are insufficient to make individual lawsuits economically feasible.

88. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Classes and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

89. The litigation of the claims brought herein is manageable. Defendant's uniform

conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

90. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

91. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

92. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Code of Civil Procedure § 382.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)

93. Plaintiffs and the Class re-allege and incorporate by reference paragraphs 1-92 as if fully set forth herein.

94. Plaintiffs and members of the Class entrusted their PII to Defendant. Defendant owed to Plaintiffs and other members of the Class a duty to exercise reasonable care in handling and using the PII in its care and custody, including by implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

95. Defendant owed a duty of care to Plaintiffs and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII—just

like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and members of the Class's PII by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

96. Defendant owed to Plaintiffs and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiffs and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiffs and members of the Class to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

97. Defendant owed these duties to Plaintiffs and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and members of the Class's personal information and PII.

98. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII—whether by malware or otherwise.

99. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiffs and members of the Class and the importance of exercising reasonable care in handling it.

100. Defendant breached its duties by failing to exercise reasonable care in supervising its

agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiffs and members of the Class which actually and proximately caused the Data Breach and Plaintiffs' and members of the Class's injury.

101. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs' and members of the Class's injuries-in-fact.

102. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and members of the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

103. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiffs and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Negligence Per Se
(On Behalf of Plaintiffs and the Class)

104. Plaintiffs and members of the Class by reference paragraphs 1-92 as if fully set forth herein.

105. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and members of the

Class's PII.

106. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, employees' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiffs' and the members of the Class's sensitive PII.

107. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect its employees' PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to its employees in the event of a breach, which ultimately came to pass.

108. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and members of the Class.

109. Defendant had a duty to Plaintiff sand the members of the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs and the Class's PII.

110. Defendant breached its respective duties to Plaintiffs and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs and members of the Class's PII.

111. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence per se.

112. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs

and members of the Class, Plaintiffs and members of the Class would not have been injured.

113. The injury and harm suffered by Plaintiffs and members of the Class were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiffs and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

114. Had Plaintiffs and members of the Class known that Defendant would not adequately protect their PII, Plaintiffs and members of the Class would not have entrusted Defendant with their PII.

115. As a direct and proximate result of Defendant's negligence per se, Plaintiffs and members of the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of their PII; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

COUNT III
Breach of an Implied Contract
(On Behalf of Plaintiffs and the Class)

116. Plaintiffs and members of the Class incorporate by reference paragraphs 1-92 as if fully set forth herein.

117. Defendant offered to employ Plaintiffs and members of the Class in exchange for their PII.

118. In turn, and through internal policies, Defendant agreed it would not disclose the PII it collects to unauthorized persons. Defendant also promised to safeguard employee PII.

///

119. Plaintiffs and the members of the Class accepted Defendant's offer by providing PII to Defendant in exchange for employment with Defendant.

120. Implicit in the parties' agreement was that Defendant would provide Plaintiffs and members of the Class with prompt and adequate notice of all unauthorized access and/or theft of their PII.

121. Plaintiffs and the members of the Class would not have entrusted their PII to Defendant in the absence of such agreement with Defendant.

122. Defendant materially breached the contract(s) it had entered with Plaintiffs and members of the Class by failing to safeguard such information and failing to notify them promptly of the intrusion into its computer systems that compromised such information. Defendant further breached the implied contracts with Plaintiff and members of the Class by:

- Failing to properly safeguard and protect Plaintiffs' and members of the Class's PII;
- Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and
- Failing to ensure the confidentiality and integrity of electronic PII that Defendant created, received, maintained, and transmitted.

123. The damages sustained by Plaintiffs and members of the Class as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

124. Plaintiffs and members of the Class have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendant.

125. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with

honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

126. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

127. Defendant failed to advise Plaintiffs and members of the Class of the Data Breach promptly and sufficiently.

128. In these and other ways, Defendant violated its duty of good faith and fair dealing.

129. Plaintiffs and members of the Class have sustained damages because of Defendant's breaches of its agreement, including breaches thereof through violations of the covenant of good faith and fair dealing.

COUNT IV
Violation of California's Consumer Records Act
Cal. Civ. Code § 1798.80, *et seq.*
(On behalf of Plaintiffs and the Class)

130. Plaintiffs and members of the Class incorporate by reference paragraphs 1-92 as if fully set forth herein.

131. Under California law, any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" must "disclose any breach of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." (Cal. Civ. Code § 1798.82.) The disclosure

must "be made in the most expedient time possible and without unreasonable delay" (*Id.*), but "immediately following discovery [of the breach], if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." (Cal. Civ. Code § 1798.82, subdiv. b.)

132. The Data Breach constitutes a "breach of the security system" of Defendant.

133. An unauthorized person acquired the personal, unencrypted information of Plaintiffs and the Class.

134. Defendant knew that an unauthorized person had acquired the personal, unencrypted information of Plaintiffs and the Class, but waited approximately three months to notify them. Three months is an unreasonable delay under the circumstances.

135. Defendant's unreasonable delay prevented Plaintiff and the Class from taking appropriate measures from protecting themselves against harm.

136. Because Plaintiffs and the Class were unable to protect themselves, they suffered incrementally increased damages that they would not have suffered with timelier notice.

137. Plaintiffs and the Class are entitled to equitable relief and damages in an amount to be determined at trial.

COUNT VI
Violation of California's Unfair Competition Law
Cal. Bus. Code § 17200, *et seq.*
(On behalf of Plaintiffs and the Class)

138. Plaintiffs and members of the Class incorporate by reference paragraphs 1-92 as if fully set forth herein.

139. For all Class members outside of the California and Georgia Subclasses, these claims are brought under the relevant consumer protection statute for the state in which they reside. For each state, the relevant statutes are as follows: Alabama-Deceptive Trade Practices Act (Ala. Code. § 8-19-1 et seq.); Alaska—Unfair Trade Practices and Consumer Protection Act (Alaska Stat.

§ 45.50.471, et seq.); Arizona—Consumer Fraud Act (Ariz. Rev. Stat. Ann. § 44-1521, et seq.); Arkansas—Deceptive Trade Practices Act (Ark. Code Ann. § 4-88-101, et seq.); Connecticut—Connecticut Unfair Trade Practices Act (Conn. Gen. Stat. § 42-110a, et seq.); Delaware—Consumer Fraud Act (Del. Code Ann. Tit. 6, § 2511, et seq.); District of Columbia— D.C. Code § 28-3901, et seq.; Florida— Deceptive and Unfair Trade Practices Act (Fla. Stat. § 501.20, et seq.); Georgia – Fair Business Practices Act of 1975 (Ga. Code § 10-1-390 et seq.);Hawaii—Haw. Rev. Stat. § 480-1, et seq.); Idaho—Consumer Protection Act (Idaho Code Ann. § 48-601, et seq.); Indiana—Deceptive Consumer Sales Act (Ind. Code § 24-5-0.5-1, et seq.); Iowa—Iowa Code § 7.14.16, et seq.); Kansas—Consumer Protection Act (Kan. Stat. Ann. § 50-623, et seq.); Kentucky—Consumer Protection Act (Ky. Rev. Stat. Ann. § 367.110, et seq.); Louisiana—Unfair Trade Practices and Consumer Protection Law (La. Rev. Stat. Ann. § 51:1401, et seq.); Maine–Unfair Trade Practices Act (Me. Stat. tit. 5, § 205-A ET SEQ.); (Maryland—Maryland Consumer Protection Act (Md. Code Ann., Com. Law § 13-101, et seq.); Massachusetts—Regulation of Business Practice and Consumer Protection Act (Mass. Gen. Laws Ann. ch. 93A, §§ 1-11); Minnesota—False Statement in Advertising Act (Minn. Stat. § 8.31, Minn. Stat. § 325F.67), Prevention of Consumer Fraud Act (Minn. Stat. § 325F.68, et seq.); Mississippi—Consumer Protection Act (Miss. Code Ann. § 75-24, et seq.); Missouri—Merchandising Practices Act (Mo. Rev. Stat. § 407.010, et seq.); Montana – Unfair Trade Practices and Consumer Protection Act of 1973 (Mont. Code Ann. § 30-14-101 et seq.); Nebraska—Consumer Protection Act (Neb. Rev. Stat. § 59-1601); Nevada—Trade Regulation and Practices Act (Nev. Rev. Stat. § 598.0903, et seq., Nev Rev. Stat. § 41.600); New Hampshire—Consumer Protection Act (N.H. Rev. Stat. Ann. § 358-A:1, et seq.); New Jersey—N.J. Stat. Ann. § 56:8-1, et seq.); New Mexico— Unfair Practices Act (N.M. Stat. § 57-12-1, et seq.); North Carolina (N.C. Gen. Stat. § 75-1.1 et seq.); North Dakota—N.D. Cent. Code § 51-15-01, et seq.); Ohio – Ohio Consumer Sales Practices Act (Ohio Rev. Code Ann.

§ 1345.01 ET SEQ.); Oklahoma—Consumer Protection Act (Okla. Stat. tit. 15, § 751, et seq.); Oregon—Unlawful Trade Practices Law (Or. Rev. Stat. § 646.605, et seq.); Rhode Island—Unfair Trade Practice and Consumer Protection Act (R.I. Gen. Laws § 6-13.1-1, et seq.); South Carolina—Unfair Trade Practices Act (S.C. Code Ann. § 39-5-10, et seq.); South Dakota—Deceptive Trade Practices and Consumer Protection Law (S.D. Codified Laws § 37-24-1, et seq.); Tennessee—Consumer Protection Act(Tenn. Code Ann. § 47- 18-101, et seq.); Utah—Consumer Sales Practices Act (Utah Code Ann. § 13-11-1, et seq.); Vermont—Consumer Fraud Act (Vt. Stat. Ann. tit. 9, § 2451, et seq.); Virginia-Consumer Protection Act of 1997 (Va. Code Ann. § 59.1-196 et seq.); Washington—Consumer Protection Act (Wash. Rev. Code § 19.86.010, et seq.); West Virginia-Consumer Credit and Protection Act (W. Va. Code § 46A-6-101 et seq.); Wisconsin— Wis. Stat. § 100.18, 100.20; Wyoming—Consumer Protection Act (Wyo. Stat. Ann. § 40-12-101, et seq.)

"Unfair" Prong

140. Under California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 et seq., a challenged activity is "unfair" when "any injury it causes outweighs any benefits provided to consumers and the injury is one that the consumers themselves could not reasonably avoid." *Camacho v. Auto Club of Southern California*, 142 Cal. App. 4th 1394, 1403 (2006).

141. Defendant's conduct as alleged herein does not confer any benefit to consumers. It is especially questionable why Defendant would continue to store individuals' data longer than necessary. Mishandling this data and a failure to archive and purge this unnecessary data shows blatant disregard for customers' privacy and security.

142. Defendant did not need to collect the private data from its consumers to allow consumers' enhanced experiences of the products or services. It did so to track and target its customers and monetize the use of the data to enhance its profits. Defendant utterly misused this

data and Private Information.

143. Defendant's conduct as alleged herein causes injuries to consumers, who do not receive a service consistent with their reasonable expectations.

144. Defendant's conduct as alleged herein causes injuries to consumers, who entrusted Defendant with their Private Information and whose Private Information was leaked as a result of Defendant's unlawful conduct.

145. Defendant's failure to implement and maintain reasonable security measures was also contrary to legislatively declared public policy that seeks to protect consumers' data and ensure entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45, California's Consumer Records Act, Cal. Civ. Code §1798.81.5, and California's Consumer Privacy Act, Cal. Civ. Code § 1798.100.

146. Consumers cannot avoid any of the injuries caused by Defendant's conduct as alleged herein.

147. The injuries caused by Defendant's conduct as alleged herein outweigh any benefits.

148. Defendant's conduct, as alleged in the preceding paragraphs, is false, deceptive, misleading, and unreasonable and constitutes an unfair business practice within the meaning of Cal. Bus. & Prof. Code § 17200.

149. Defendant could have furthered its legitimate business interests in ways other than by unfair conduct.

150. Defendant's conduct threatens consumers by exposing consumers' Private Information to hackers. Defendant's conduct also threatens other companies, large and small, who play by the rules. Defendant's conduct stifles competition and has a negative impact on the marketplace and reduces consumer choice.

151. All of the conduct alleged herein occurs and continues to occur in Defendant's

business. Defendant's wrongful conduct is part of a pattern or generalized course of conduct.

152. Pursuant to Cal. Bus. & Prof. Code § 17203, Plaintiffs and the Class Members seek an order of this Court enjoining Defendant from continuing to engage, use, or employ its unfair business practices.

153. Plaintiffs and the Class Members have suffered injury-in-fact and have lost money or property as a result of Defendant's unfair conduct. Plaintiffs relied on and made their decision to use Defendant's services in part based on Defendant's representations regarding their security measures and trusted that Defendant would keep their Private Information safe and secure. Plaintiffs accordingly provided their Private Information to Defendant reasonably believing and expecting that their Private Information would be safe and secure. Plaintiffs paid an unwarranted premium for the purchased services. Specifically, Plaintiffs paid for services advertised as secure when Defendant in fact failed to institute adequate security measures and neglected vulnerabilities that led to a data breach. Plaintiffs and the Class Members would not have purchased the services, or would not have given Defendant their Private Information, had they known that their Private Information was vulnerable to a data breach. Likewise, Plaintiffs and the members of the Class seek an order mandating that Defendant implement adequate security practices to protect consumers' Private Information. Additionally, Plaintiffs and the Class Members seek and request an order awarding Plaintiffs and the Class restitution of the money wrongfully acquired by Defendant by means of Defendant's unfair and unlawful practices.

"Unlawful" Prong

154. Cal. Bus. & Prof. Code § 17200, et seq., identifies violations of any state or federal law as "unlawful practices that the unfair competition law makes independently actionable." *Velazquez v. GMAC Mortg. Corp.*, 605 F. Supp. 2d 1049, 1068 (C.D. Cal. 2008).

///

155. Defendant's unlawful conduct, as alleged in the preceding paragraphs, violates Cal. Bus. & Prof. Code § 1750 et seq.

156. Defendant's conduct, as alleged in the preceding paragraphs, is false, deceptive, misleading, and unreasonable and constitutes unlawful conduct.

157. Defendant has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, et seq., the FTC Act, 15 U.S.C. § 45, and California common law. Defendant failed to notify all of its affected customers regarding said breach, failed to take reasonable security measures, or comply with the FTC Act, and California common law.

158. Defendant knew or should have known of its unlawful conduct.

159. As alleged in the preceding paragraphs, the misrepresentations by Defendant detailed above constitute an unlawful business practice within the meaning of Cal. Bus. & Prof. Code §17200.

160. Defendant could have furthered its legitimate business interests in ways other than by its unlawful conduct.

161. All of the conduct alleged herein occurs and continues to occur in Defendant's business. Defendant's unlawful conduct is part of a pattern or generalized course of conduct.

162. Pursuant to Cal. Bus. & Prof. Code § 17203, Plaintiffs and the Class seek an order of this Court enjoining Defendant from continuing to engage, use, or employ its unlawful business practices.

163. Plaintiffs and the Class have suffered injury-in-fact and have lost money or property as a result of Defendant's unfair conduct. Plaintiffs paid an unwarranted premium for services.

Specifically, Plaintiffs paid for services advertised as secure when Defendant in fact failed to institute adequate security measures and neglected vulnerabilities that led to a data breach. Plaintiffs and the Class Members would not have purchased the products and services, or would not have given Defendant their Private Information, had they known that their Private Information was vulnerable to a data breach. Likewise, Plaintiffs and the members of the Class seek an order mandating that Defendant implement adequate security practices to protect consumers' Private Information. Additionally, Plaintiffs and the Class Members seek and request an order awarding Plaintiffs and the Class Members restitution of the money wrongfully acquired by Defendant by means of Defendant's unfair and unlawful practices.

COUNT VII

Violation of the California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.150
(On behalf of Plaintiff Finch, Plaintiff Sampson, and the California Subclass)

164. Plaintiff Finch and Plaintiff Sampson and members of the California Subclass incorporate by reference paragraphs 1-92 as if fully set forth herein.

165. Defendant violated California Civil Code § 1798.150 of the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the nonencrypted PII of Plaintiff Finch and Plaintiff Sampson and the California Subclass. As a direct and proximate result, Plaintiff Finch's and Plaintiff Sampson's, and the California Subclass 's nonencrypted and nonredacted PII was subject to unauthorized access and exfiltration, theft, or disclosure.

166. Defendant is a business organized for the profit and financial benefit of its owners according to California Civil Code § 1798.140, that collects the personal information of its employees and whose annual gross revenues exceed the threshold established by California Civil Code § 1798.140(d).

167. Plaintiff Finch and Plaintiff Sampson ("Plaintiffs" for the remainder of this

allegation) and California Subclass members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold PII, including Plaintiff Finch's, Plaintiff Samson's and California Subclass members' PII. Plaintiffs and California Subclass members have an interest in ensuring that their PII is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information.

168. Pursuant to California Civil Code § 1798.150(b), Plaintiff Finch and Plaintiff Sampson sent CCPA notice letters to Defendant, detailing the specific provisions of the CCPA that Defendant has violated and continues to violate.

169. Defendant timely responded to Plaintiffs' CCPA notices but did not actually cure the noticed violations. Defendant asserted, without evidence or proof, that it "cured" the above failures to implement reasonable security procedures to prevent unauthorized access of Plaintiffs' and California Subclass members' PII by discussing the post attack actions it allegedly took, which did not retroactively cure the unauthorized access, as Defendant provides no assurance that Plaintiffs' and California Subclass members' PII is not still in the hands of unauthorized third parties.

170. Furthermore, none of the steps Defendant asserts in its CCPA responses demonstrate an actual cure of its failure to implement reasonable security measures to protect Plaintiffs' and California Subclass members' PII as the steps it asserts it has taken are not sufficient to protect Plaintiffs' and California Subclass members' PII.

171. Defendant's response is wholly insufficient to demonstrate any "actual cure" of its failure to implement reasonable security to protect the information.

172. As Defendant has not "actually cured" the violation, Plaintiffs and the California Subclass seek statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident, or actual damages,

whichever is greater. See Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

COUNT VII
Violation of Georgia Uniform Deceptive Trade Practices Act
Ga. Code Ann §§ 10-1-370, et seq.
(On Behalf of Plaintiff Donelson and Georgia Subclass)

173. Plaintiff Samantha Donelson individually and on behalf of the Georgia Subclass incorporate by reference paragraphs 1-92 as if fully set forth herein.

174. Pursuant to O.C.G.A. § 13-6-11, the jury may allow the expenses of litigation and attorneys' fees as part of the damages where a defendant "has acted in bad faith, has been stubbornly litigious, or has caused the plaintiff unnecessary trouble and expense."

175. Defendant through its actions alleged and described herein acted in bad faith, were stubbornly litigious, or caused the Georgia Subclass unnecessary trouble and expense with respect to the transaction or events underlying this litigation.

176. The Georgia Subclass therefore requests that their claim for recovery of expenses of litigation and attorneys' fees be submitted to the jury, and that they Court enter a Judgement awarding their expenses of litigation and attorneys' fees pursuant to O.C.G.A. § 13-6-11.

PRAYER FOR RELIEF

Plaintiffs and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiffs and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiffs and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

DEMAND FOR JURY

Plaintiffs demand a trial by jury on all issues so triable.

Date: April 4, 2023

Respectfully Submitted,

/s/ Michael J. Boyle, Jr.

Matthew R. Wilson (Bar No. 290473)
mwilson@meyerwilson.com
Michael J. Boyle, Jr. (Bar No. 258560)
mboyle@meyerwilson.com
MEYER WILSON CO., LPA
305 W. Nationwide Boulevard
Columbus, OH 43215
Telephone: (614) 224-6000
Facsimile: (614) 224-6066

M. Anderson Berry (SBN 262879)
aberry@justice4you.com
Gregory Haroutunian (SBN 330263)
gharoutunian@justice4you.com
CLAYEO C. ARNOLD,
A PROFESSIONAL CORPORATION

865 Howe Avenue
Sacramento, CA 95825
Telephone: (916)239-4778
Fax: (916) 924-1829

John J. Nelson (SBN 317598)
jnelson@milberg.com
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
401 W Broadway, Suite 1760
San Diego, California 92101
Telephone: (858) 209-6941

Samuel J. Strauss *(Pro Hac Vice forthcoming)*
sam@turkestrauss.com
Raina Borrelli *(Pro Hac Vice forthcoming)*
raina@turkestrauss.com
TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, WI 53703
Telephone: 608-237-1775

Attorneys for Plaintiffs and the Proposed Class